IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SEALORD HOLDINGS, INC., SEALORD LLC, and FIRST SEALORD SURETY, INC.,	:	
Plaintiffs,	:	CIVIL ACTION
v.	:	
JOSEPH RADLER,	:	NO. 11-6125
Defendant.	:	

MEMORANDUM

ROBERT F. KELLY, Sr. J. **MARCH 6 , 2012**

Presently before the Court is Defendant, Joseph Radler's ("Radler"), Motion to Dismiss Plaintiffs, Sealord Holdings, Inc. ("Sealord Holdings"), Sealord LLC, and First Sealord Surety, Inc.'s ("FSSI") (collectively, "Sealord"),[1] Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). For the reasons stated below, we will grant the Motion, but grant Sealord leave to amend its Complaint in accordance with this Memorandum Opinion.

I. PROCEDURAL AND FACTUAL HISTORY

Radler is a former employee of Sealord. He began his employment with FSSI as the Chief Technology Officer ("CTO") on October 21, 2009. (Compl. ¶ 11.) Radler worked in this capacity until he resigned effective 5:00 p.m. on July 26, 2011. (Id.) Sealord asserts that as CTO, Radler had knowledge of, and dominion and control over FSSI's computer systems, and the information contained in them, including confidential, proprietary and trade secret

[1]Sealord LLC is a Delaware limited liability company. (Compl. ¶ 4.) Sealord Holdings is a Pennsylvania holding corporation and is owned by Sealord LLC. (Id. ¶ 5.) FSSI is a Pennsylvania corporation in the business of issuing surety bonds and is owned by Sealord Holdings. (Id. ¶ 6.)

information. (Id. ¶¶ 11- 13.) Sealord alleges that because of Radler's in-depth knowledge of its computer systems, where the vast majority of the company's confidential information is stored, Radler had the potential to access, obtain, and disseminate the entirety of this information. (Id. ¶ 13.) Sealord asserts that by virtue of Radler's assistance to its executives in using the computer network system, including the Chief Financial Officer ("CFO"), who is Radler's brother-in-law, Radler knew the user names and passwords for these executives' computers, including the CFO's computer. (Id.)

Sealord states that some of the information that Radler was made privy to included highly confidential information concerning a "potential merger, sale, or similar transaction" ("Transaction"). (Id. ¶ 14.) Sealord avers that prior to Radler's resignation in March 2011, it began to contemplate this potential Transaction, and engaged Dowling Hales ("Hales"), an investment banking firm in New York, to act as its financial advisor to assist in the potential Transaction. (Id. ¶ 15.) Hale introduced a number of potential participants to Sealord for a proposed Transaction, each of whom signed confidentiality/non-disclosure agreements with Sealord (the "Suitors").[2] (Id.) Sealord states that it took appropriate measures to ensure that negotiations were kept confidential and not disclosed outside a small circle of individuals in its company, including Radler. (Id. ¶ 16.) Sealord continued to pursue the potential Transaction after Radler left the company. (Id.)

Two days after Radler left Sealord, Radler contacted Sealord and demanded payment for

[2]Sealord states in its Complaint that "due to the highly confidential nature of Sealord's ongoing negotiations and/or plans in connection with the Transaction, the Suitors will not be mentioned by name in this Complaint. Rather, they will instead be referred to by the aliases of 'Confidential Suitor #1' and 'Confidential Suitor #2.'" (Id. at 2, n.1.) We will do the same in this Memorandum Opinion.

vacation time and bonus. (Id. ¶ 26.) On August 4, 2011, Sealord told Radler that, consistent with the company's policies, he was not entitled to payments for bonus or vacation time. (Id. ¶ 27.) Sealord asserts that eight days after it informed Radler that he was not entitled to the monies claimed, Confidential Suitor #1 received an anonymous typewritten note warning this suitor about the pitfalls of entering into the Transaction with Sealord. (Id. ¶ 28.) The typewritten note was addressed to two executives of Confidential Suitor #1 whose names were associated with the Transaction in Sealord's confidential computer files, including those on the CFO's computer. (Id.) Sealord learned about this anonymous note on September 7, 2011, and on that same day, Confidential Suitor #1 also advised it that it had received an email sent on August 31, 2011, from Sealordlies@gmail.com warning it about making "large purchases." (Id. ¶ 29.) It was sent to the leading officer of Confidential Suitor #1 whose name was associated with the Transaction in Sealord's confidential computer files, including those on the CFO's computer. (Id.)

On September 12, 2011, Sealord learned that another disparaging email was sent on September 11, 2011, from bondsclaims@yahoo.com to most of the due diligence team from Confidential Suitor #1, as well as the lead officer at Confidential Suitor #2, warning about Sealord's operating practices and questioning its integrity. (Id. ¶ 30.) This same email was also sent to the Deputy Commissioner at the Pennsylvania Department of Insurance who is the principal regulator of FSSI, and to a competitor in California with whom FSSI recently had a dispute. (Id.) This confidential information was in Sealord's confidential computer files, including those on the CFO's computer. (Id.)

Sealord asserts that the words in the September 11, 2011 emails from this address closely mirrored those contained in an internal email sent by Sealord's Executive Vice President on

September 9, 2011, to only four other executives at FSSI, including the CFO. (Id. ¶ 32.) Sealord avers that on September 12, 2011, it learned that another email from this same address had been sent to the lead officer at Confidential Suitor #1 and the investment banker for Confidential Suitor #2 urging caution in proceeding with the Transaction with FSSI. This confidential information was in Sealord's computer files. (Id. ¶ 33.) On September 12, 2011, Sealord learned from Confidential Suitor #2 that it had received a typewritten letter from an anonymous source, addressed to its President of Commercial Lines, alleging inflated value and revealing Sealord's negotiations with a prior suitor. (Id. ¶ 34.) The identity of this prior suitor and the identity of Confidential Suitor #2 were confidential information that was kept in Sealord's computer files, including in those files kept on the CFO's computer. (Id. ¶ 35.)

Sealord asserts that at this point, a total of four disparaging emails and two typewritten notes had been received by its potential business partners, competitors, and regulating authorities, and such had an impact upon its relationship with its potential suitors. (Id. ¶ 34.) On September 12, 2011, Confidential Suitor #1 withdrew from negotiations on the Transaction, and on September 19, 2011, Confidential Suitor #2 withdrew from the Transaction. (Id. ¶ 36.)

With serious concerns about these emails, Sealord hired Lexington Technology Auditing, Inc. ("Lexington") to conduct an investigation and damage assessment. (Id. ¶ 37.) On September 13, 2011, the day after Lexington was hired, certain members of Sealord's Board of Directors received an email purportedly sent from the America Online account of one of its former employees (not Radler), verbally attacking the competence and leadership of Sealord's senior management. (Id. ¶ 38.) Sealord received no further contact from this email address, and believed that the email was not sent by the former employee. (Id.) Lexington investigated the

email address and discovered that it was registered to a BTK Communications, Inc. ("BTK") with an address of 684 Korisa Drive, Lower Moreland, Pennsylvania. (Id. ¶ 39.) The website of BTK lists Radler's wife as the company principal with this same address. This address is also Radler's home address. (Id.)

Sealord asserts further that this same day, Lexington also learned that Sealord's executives had not changed their passwords in over a year, and because of this, it changed the passwords of certain Sealord employees, including the CFO, Radler's brother-in-law. (Id. ¶ 40.) Sealord alleges that within an hour of the changing of the CFO's password, there were two failed attempts to access this computer, and during this same time frame, Radler unexpectedly telephoned the CFO who was in his office. (Id.) The CFO immediately reported this call to Lexington who found out that the Internet Protocol Address ("IP") of the source of the computer attempting to access the CFO's computer was a location in Huntington Valley, Pennsylvania, which was located approximately 800 yards from Radler's address. (Id.) No other employees of Sealord reside in that vicinity. (Id.)

Sealord also asserts that Lexington conducted a damage assessment of its compromised computer system which has resulted in damages and that it continues to suffer damages in the future. (Id. ¶¶ 42-44.) Sealord avers that "[b]ecause Defendant accessed Sealord's computer systems without authorization and then disclosed the proprietary and confidential information that he obtained via his unauthorized access, Sealord has suffered and continues to suffer an impairment to the integrity and availability of its computer files, programs, systems, source code, equipment, and other information, data, and property." (Id. at 51.)

In its Complaint, Sealord asserts violations of the Computer Fraud and Abuse Act, 18

U.S.C. § 1030 et seq. ("CFAA"). Specifically, Sealord claims violations of 18 U.S.C. §§ 1030(a)(2)(c) and (a)(4) of the CFAA. Sealord also asserts state law claims for breach of contract, misappropriation of trade secrets under 12 Pa. C.S. 5301, et seq., conversion, and tortious interference with prospective economic advantage. On September 28, 2011, Sealord filed a Motion for Temporary Restraining Order and Preliminary Injunction. This Court held a hearing on this Motion on October 7, 2011. During the hearing, the parties negotiated and agreed to the terms of an Interim Consent Order which we subsequently signed on October 14, 2011, and made part of the record. (Doc. No. 16-17). Radler filed the instant Motion to Dismiss the Complaint on November 17, 2011. Sealord responded on January 3, 2012, and Radler filed a Reply on January 24, 2012.

II. STANDARD OF REVIEW

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests the sufficiency of a complaint. Kost v. Kozakiewicz, 1 F.3d 176, 183 (3d Cir. 1993). Under Rule 12(b)(6), the defendant bears the burden of demonstrating that the plaintiff has not stated a claim upon which relief can be granted. Fed. R. CIV. P. 12(b)(6); see also Hedges v. United States, 404 F.3d 744, 750 (3d Cir. 2005). In Bell Atl. Corp. v. Twombly, the Supreme Court stated that "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." 550 U.S. 544, 555 (2007). Following Twombly, the Third Circuit has explained that the factual allegations in the complaint may not be "so undeveloped that it does not provide a defendant the type of notice which is contemplated by Rule 8." Phillips v. County of Allegheny, 515 F.3d 224, 233 (3d Cir. 2008). Moreover, "it is no longer sufficient to allege mere elements of a cause of

action; instead 'a complaint must allege facts suggestive of [the proscribed] conduct.'" Id. (alteration in original) (quoting Twombly, 550 U.S. at 563 n.8). Furthermore, the complaint's "factual allegations must be enough to raise a right to relief above the speculative level." Id. at 234 (quoting Twombly, 550 U.S. at 555). "This 'does not impose a probability requirement at the pleading stage,' but instead 'simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element.'" Id. (quoting Twombly, 550 U.S. at 556).

Notwithstanding Twombly, the basic tenets of the Rule 12(b)(6) have not changed. The Knit With v. Knitting Fever, Inc., No. 08-4221, 2009 U.S. Dist. LEXIS 30230, at *6 (E.D. Pa. Apr. 8, 2009). The general rules of pleading still require only a short and plain statement of the claim showing that the pleader is entitled to relief, not detailed factual allegations. Phillips, 515 F.3d at 231. Moreover, when evaluating a motion to dismiss, the court must accept as true all well-pleaded allegations of fact in the plaintiff's complaint, and must view any reasonable inferences that may be drawn therefrom in the light most favorable to the plaintiff. Id.; Buck v. Hampton Twp. Sch. Dist., 452 F.3d 256, 260 (3d Cir. 2006). Finally, the court must "determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." Pinkerton v. Roche Holdings Ltd., 292 F.3d 361, 374 n.7 (3d Cir. 2002).

III. DISCUSSION

1. CFAA Claims

Radler asserts that Sealord's CFAA claims should be dismissed because "the allegations concerning Radler's culpability for the communications are based on pure speculations," and "Sealord failed to plead facts sufficient to support three prerequisites to claims asserted under

CFAA §§ 1030(a)(2)(C) and (a)(4)." (Def.'s Mot. Dismiss at 7.)

The CFAA, while primarily a criminal statute, provides a civil cause of action in § 1030(g).[3] To state a civil claim for a violation of the CFAA, a plaintiff must allege: 1) damage or loss; 2) caused by; 3) a violation of one of the substantive provisions set forth in § 1030(a); and 4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)-(V).[4] 18 U.S.C. § 1030(g). Sealord asserts that it has adequately pled all these elements.

---

[3] This section states in its entirety:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g).

[4]Subsection (g) requires civil litigants to allege one of the following five effects set forth in § 1030(a)(5)(B):

> (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security[.]

18 U.S.C. § 1030(a)(5)(B).

A. Whether Sealord Has Properly Pled Damages Under the CFAA

Radler first asserts that Sealord has failed to plead "damage" to its computer system, or a "loss" within the meaning of §§ 1030(e)(8) or (e)(11). The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The statute goes on to define "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Numerous district court decisions in the Third Circuit have held that to fall within this definition of "loss," the "alleged 'loss' must be related to the impairment or damage to a computer or computer system." Fontana v. Curry, No. 10-1685, 2011 WL 4473285, at *7 (W.D. Pa. Aug. 30, 2011); see also Eagle v. Morgan, No. 11-4303, 2011 WL 6739448, at *8 (E.D. Pa. Dec. 22, 2011); Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, No. 08–2751, 2010 WL 4224473, at *6 (E.D. Pa. Oct. 22, 2010) ("Various courts have interpreted 'loss' to mean the remedial costs of investigating a computer for damage, remedying damage done, and costs incurred while the computer is inoperable."). Likewise, courts have found that lost revenue incurred because of an interruption of service falls within the definition of "loss." Fontana, 2011 WL 4473285, at *7; Eagle, 2011 WL 6739448, at *8. Claims of lost business opportunities, damaged reputation, loss of assets, and other missed revenue, however, do not constitute "loss." See e.g., Fontana, 2011 WL 4473285, at *8; (finding that a claim for future lost revenue due to the dissemination of trade secrets was not a "loss" under the CFAA); Crown Coal & Coke Co. v.

Compass Point Res., LLC, No. 07–1208, 2009 WL 1806659, at *8 (W.D. Pa. June 23, 2009) (holding that alleged loss of business opportunities not compensable under the CFAA); Advantage Ambulance Grp. v. Lugo, No. 08–330, 2009 WL 839085, at *4 (E.D. Pa. Mar. 30, 2009) (finding that allegation of a "loss of revenue" is not the type of loss encompassed by the CFAA).

"A compensable 'loss' under the CFAA, therefore, is a loss which is in some way related to functionality of the protected computer at issue. Either the loss is the cost of remedial measures taken to investigate or repair the damage to the computer, or the loss is the amount of lost revenue resulting from a plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance." Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio, No. 09-2751, 2011 WL 6088611, at *4-5 (E.D. Pa. Dec. 7, 2011); see also Telquest Intern., Corp. v. Dedicated Business Systems, Inc., No. 06-5359, 2009 WL 3234226, at *2 (D. N.J. Sept. 30, 2009); Chas S. Winter, Inc. v. Polistina, No. 06-4865, 2007 WL 1652292, at *1 (D. N.J. June 4, 2007).

Sealord states in its Response that it recognizes that there are district court decisions in this Circuit that determined that the investigating or remedying damage must be related to the damage to the computer or due to interruption of the computer's service. (Pls.' Resp. Mot. Dismiss at 22.) Nonetheless, Sealord takes the position that it is sufficient to bring a cause of action under the CFAA by merely alleging any type of costs responding to Radler's misappropriation of its computer data. See P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, LLC., No. 04-4554, 2007 WL 708978, at *1 (D. N.J. Mar. 5, 2007); see also EF Cultural Travel BV, EF v. Explorica, Inc., 274 F.3d 577, 584-85 (1st Cir. 2001);

Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000).

Here, we will follow the district court decisions in our Circuit which have held that the investigating or remedying damage must be related to the damage to the computer or due to interruption of the computer's service. See, e.g., Fontana, 2011 WL 4473285, at *7; Eagle, 2011 WL 6739448, at *8; Clinton Plumbing & Heating of Trenton, Inc., 2010 WL 4224473, at *4-5. Sealord argues that even if we follow the holdings in these cases, it has still pled that it suffered both computer damage and interruption of its computer services and, therefore, has adequately pled a CFAA cause of action. (Pls.' Resp. Mot. Dismiss at 22.) Sealord also states that "[i]f this Court agrees that the investigative and remedial costs must be related to damage to the computer or the interruption of computer service, and if this Court finds that Plaintiffs have not adequately pled damage to its computer systems or interruption of computer service, Plaintiffs request that this Court grant Plaintiffs leave to amend its Complaint." (Id. at 22, n. 114.) Here, we find that Sealord has not adequately pled such damage. However, we will grant its request to amend its Complaint to adequately plead damage to its computers and/or interruption of its computer service.

As noted, Sealord avers that Radler accessed its computers with intent to defraud, and this fraud included Radler's scheme to steal its confidential and proprietary information by using misappropriated passwords and disclosure of its files via anonymous letters and emails. (Compl. ¶¶ 62-63.) Sealord claims that Radler's actions "caused damage and loss to Sealord's computer files, programs, systems, information, equipment, data, or other property by accessing, altering and deleting same." (Id. ¶ 66.) Sealord further avers that it has "expended sums in excess of

$5000 for its computer forensic consultant to conduct an assessment of how much damage has been done to the Sealord computers that Defendant accessed. The assessment of damages to the computer systems includes assessment of permanently deleted files, programs, and usage history." (Id. ¶ 68.) Sealord also claims that it has "experienced lost revenue, costs, and other consequential damages in excess of $5000 as a result of the interruption of service it experienced as a result of the unauthorized access." (Id. ¶ 69.)

We are of the opinion that while Sealord does aver general damage to its computers and interruption of service, such averments are not specific enough to satisfy the requirements of Twombly, 550 U.S. at 556, and Federal Rule of Civil Procedure 12(b)(6). As stated earlier, following Twombly, the United States Court of Appeals for the Third Circuit has explained that the factual allegations in the complaint may not be "so undeveloped that it does not provide a defendant the type of notice which is contemplated by Rule 8." Phillips, 515 F.3d at 233. Moreover, "it is no longer sufficient to allege mere elements of a cause of action; instead 'a complaint must allege facts suggestive of [the proscribed] conduct.'" Id. (quoting Twombly, 550 U.S. at 563 n.8). Accordingly, we will grant Radler's Motion to Dismiss, but grant Sealord leave to amend the Complaint to comply with the tenets of Twombly and Rule 12(b)(6).

B. Whether Sealord Has Adequately Pled "Intent to Defraud" Under the CFAA

Sealord avers liability under § 1030(a)(4). This section imposes civil liability upon one whom:

> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of

such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4). The Third Circuit stated in P.C. Yonkers, Inc. v. Celebrations! the Party & Seasonal Superstore, LLC. that: a claim under CFAA § 1030(a)(4) has four elements: (1) defendant has accessed a "protected computer;" (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so "knowingly" and with "intent to defraud;" and (4) as a result has "further[ed] the intended fraud and obtain[ed] anything of value." 428 F.3d 504, 508 (3d Cir. 2005).

Radler argues that Sealord has failed to plead "intent to defraud with sufficient specifically to maintain an action under § 1030(a)(4)." (Def.'s Mot. Dismiss at 22.) Sealord responds that they need only aver the intent to defraud element of its CFAA claims generally, and that it has done so in its Complaint. See P.C. of Yonkers, Inc., 2007 WL 708978, at *6. We agree with Sealord. In Yonkers, the defendants argued that plaintiffs failed to state a claim under the CFAA in their complaint because they did not, in accordance with Federal Rule of Civil Procedure 9(b), allege with sufficient specificity that defendants intended to defraud them. (Id.) Yonkers held that "[c]ontrary to Defendants' contention, in order to state a claim under the CFAA, Plaintiffs need only allege the required elements, pursuant to Rule 8(a)(2)'s notice-pleading standard."[5] The court in Yonkers further held that "[d]espite the fact that the CFAA

[5]Federal Rule of Civil Procedure 8(a) states:

> [a] pleading which sets forth a claim for relief, whether an original claim, counterclaim, cross-claim, or third-party claim, shall contain (1) a short and plain statement of the grounds upon which the court's jurisdiction depends, unless the court already has jurisdiction and the claim needs no new grounds of jurisdiction to support it, (2) a short and plain statement of the claim showing that the pleader is entitled to relief, and (3) a demand for judgment for the relief the pleader seeks. Relief in the alternative or of several different types may be demanded.

contains the term 'fraud,' Rule 9(b)'s[6] heightened pleading standard does not apply to claims made under the statute." Id.; see also Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro, No. 3:09-2175, 2007 WL 1847435, at *7 (M.D. Pa. June 25, 2007); Lockheed Martin Corp. v. Speed, No. 6:05-1580, 2006 WL 2683058, at *3 (M.D. Fla. Aug. 1, 2006); C.H. Robinson Worldwide, Inc. v. Command Transp., LLC, No. 05 C 3401, 2005 WL 3077998, at *4 (N.D. Ill. Nov. 16, 2005).

Here, we are of the opinion that Sealord has sufficiently pled intent to defraud to state a claim under the CFAA and satisfy the notice-pleading requirements of Rule 8(a)(2). Sealord specifically avers that "[u]pon information and belief, Defendant has been intentionally accessing Sealord's computer systems, computer files, computer information, and computer data, without authorization and with specific intent to defraud Sealord." (Compl. ¶ 46.) Moreover, as outlined above, Sealord has averred specific allegations of unlawful and deceitful actions on the part of Radler which were committed with the intent to defraud Sealord. Thus, Radler's argument that Sealord has failed to adequately plead "intent to defraud" is without merit.

C. Whether Sealord Has Adequately Pled that Radler "Accessed" its Computers

Next, Radler argues that Sealord has failed to plead that he "accessed" its computers within the meaning and intent of the Act. (Def.'s Mot. Dismiss, at 25.) In addition, Radler

---

Fed. R. Civ. P. 8(a).

[6]Federal Rule of Civil Procedure 9(b) provides:

> In all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity. Malice, intent, knowledge, and other condition of mind of a person may be averred generally.

Fed. R. Civ. P. 9(b).

asserts that there are no allegations in the Complaint which specifically aver that he is the person who gained entry into Sealord's computers, and there are no allegations about how he gained access. (Id. at 28-29.) We disagree.

In Integrated Waste Solutions, Inc. v. Goverdhanam, the defendant argued in a motion to dismiss that plaintiff failed to identify the IP addresses of the computers allegedly accessed or the persons who purportedly accessed the computers, the dates of access, or the information accessed. No. 10-2155, 2010 WL 4910176, at *9 (E.D. Pa. Nov. 30, 2010). The court, noting that defendant failed "to cite any authority naming these factors as essential to a CFAA claim," found that plaintiff had stated a plausible claim under the CFAA, and denied the motion to dismiss. Id. Likewise, Radler does not cite to any case law which holds that Sealord was required to specifically identify him as the person who accessed Sealord's computers and/or how he specifically gained access to its computer system in order to sufficiently plead a claim under the CFAA. In fact, Radler acknowledges that the word "access" is not defined in the statute, and that "[n]o circuit courts have addressed the definition, and only a small number of District Courts have addressed the definition the word 'access' without doing so in conjunction with the words 'without authorization.'" (Pl.'s Resp. Mot. Dismiss at 25.)

Moreover, Sealord has pled that it has identified an IP address of the computer that sent an anonymous email to members of its Board of Directors attacking the competence and leadership of its senior management as BTK Communications which lists Radler's wife as the company's principal with Radler's home address. (Compl. ¶ 39.) In addition, Sealord has alleged that it has identified the IP address of a computer that attempted to access its computer systems an hour after its passwords were changed as an address located very close to Radler's

home. (Id. at 40.) We, thus, find that Sealord has sufficiently pled that Radler had "accessed" its computers.[7]

IV. CONCLUSION

We find that Sealord has not sufficiently pled "damage" and "loss" in its Complaint to state a cause of action under 18 U.S.C. § 1030(g). However, we grant Sealord leave to amend its Complaint to satisfy the requirements of this Section in accordance with this Memorandum Opinion. In addition, we find that Sealord has adequately pled causes of action under the CFAA's substantive provisions set forth in 18 U.S.C. § 1030(a). Accordingly, we grant Radler's Motion to Dismiss, and grant Sealord leave to amend its Complaint.

An appropriate Order follows.

[7]Lastly, Radler argues that if we dismiss the CFAA claims, we should exercise our discretion and decline to exercise supplemental jurisdiction over Sealord's remaining state law claims. (Def.'s Mot. Dismiss at 30.) However, because we are dismissing the Complaint, but giving Sealord leave to amend to sufficiently plead "damage" and "loss" under the statute, we will address this issue upon review of the amended complaint.